



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,422	02/22/2002	Alan Rubinstein	3COM-3721.BCG.US.P	3780

7590 11/18/2004
WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER

PHU, SANH D

ART UNIT	PAPER NUMBER
2682	4

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/082,422

Applicant(s)

RUBINSTEIN ET AL.

Examiner

Sanh D Phu

Art Unit

2682

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2&3.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Art Unit: 2682

DETAILED ACTION

Information Disclosure Statement

1. The IDS filed 9/26/2003 and 7/22/2004 have been considered and recorded in the file.

Claim Rejections – 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claim 1–5, 7–16, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al (6,796,490) in view of Rioz et al (WO 01/17310).

As per claim 1, see Drummond et al Fig. 4 and 5, col. 6, line 18 to col. 9, line 22, Drummond et al disclose a method for managing wireless access to a network, comprising:

Art Unit: 2682

providing wireless communication in a network (120) (se Fig. 5);

providing a firewall (126) protection between said network (120) and a wireless access device (136, 138, 140) (see Fig. 5);

submitting an identification code (User ID) to said network from said wireless access device (see col. 6, line 61);

determining the validity of said identification code (see col. 6, lines 66–67);

granting wireless network access to said wireless access device when said identification code is valid (se col. 7, lines 1–2);

He does not disclose denying network access if identification code is invalid, however, he has a function for checking error logs (see col. 9, line 16).

Rioz et al disclose that denying wireless network access to said wireless access device when said identification code is not valid (see fig. 3, page 12, lines 2–5); and

issuing an alert when said identification code is not valid (see Fig. 3, page 12, lines 5–7).

Art Unit: 2682

Therefore, at the time of the invention was made, it would have been obvious for one skilled in the art to implement the authentication identity, as taught by Rioz et al, in order to have a fully access network protection so that computer hackers or unauthorized person can not access to the wireless network.

As per claim 2, Drummond et al disclose the method wherein said providing said wireless communication is accomplished with a wireless HUB enabled for wireless communication (see Fig. 5).

As per claim 3, Drummond et al disclose the method wherein said providing said wireless communication is accomplished in circuitry resident in said wireless HUB ((124) has a circuit device which is IEEE802.11 or Blue-tooth or any IR to interface with wireless access device) (see Fig. 5, col. 7 lines36-51).

As per claim 4, Drummond et al disclose the method wherein said identification code is the media access control number (User ID, password) of said wireless access device (see col. 6, line 66 to col. 7, line 1).

As per claim 5, Drummond et al disclose the method wherein said determining said validity of said identification code is accomplished by

Art Unit: 2682

reference to a List of valid identification codes (122) (identifying device) (see Fig. 5).

As per claim 7, Drummond et al disclose the method wherein said list of valid identification codes is resident in a server in said network (see Fig. 5).

As per claim 8, Drummond et al disclose the method wherein said denying said wireless access to said network is accomplished simultaneously with granting access to wireless access devices with valid identification codes (see Fig. 4 and 5, col. 6, line 18 to col. 9, line 22).

As per claim 9, Drummond et al disclose the method wherein said network is a wireless personal area networks (120) (see Fig. 5).

As per claim 10, Drummond et al disclose a computer network, comprising:

a Server (128) (see Fig. 5);

a wireless connection device (124) communicatively coupled with said server (see Fig. 5);

Art Unit: 2682

a wireless access device (136,138,140) enabled to wirelessly submit an identification code (User ID) to said wireless connection device (see Fig. 4 and 5, col. 6, line 18 to col. 9, line 22); and

granting wireless network access to said wireless access device when said identification code is valid (see col. 7, lines 1-2);

He does not disclose denying network access if identification code is invalid, however, he has a function for checking error logs (see col. 9, line 16).

Rioz et al disclose that denying wireless network access to said wireless access device when said identification code is not valid (see fig. 3, page 12, lines 2-5); and

issuing an alert when said identification code is not valid (see Fig. 3, page 12, lines 5-7).

Therefore, at the time of the invention was made, it would have been obvious for one skilled in the art to implement the authentication identity, as taught by Rioz et al, in order to have a fully access network protection so that computer hackers or unauthorized person can not access to the wireless network.

Art Unit: 2682

As per claim 11, Drummond et al disclose the computer network wherein said server is an Internet portal (internet gateway or Proxy server) (see Fig. 4 and 5).

As per claim 12, Drummond et al disclose the computer network wherein said wireless connection device is a wireless HUB enabled for wireless communication (see Fig. 4 and 5).

As per claim 13, Drummond et al disclose the computer network wherein said wireless access device is a wirelessly enabled laptop computer (138) (see Fig. 5).

As per claim 14, Drummond et al disclose the computer network wherein said wireless access device is a wirelessly enabled personal data assistant (136) (see Fig. 5).

As per claim 15, Drummond et al disclose the computer network wherein said wireless access device is a wireless telephone enabled for data communication (140) (see Fig. 5).

Art Unit: 2682

As per claim 16, Drummond et al disclose the computer network wherein said wireless access device is a wirelessly enabled computer peripheral device (IEEE 802.1, Bluetooth, IR) (see Fig. 5).

As per claim 18, Drummond et al disclose the computer network wherein said distributed firewall is enabled to obtain a List of valid identification codes from said server (see Fig. 5).

As per claim 19, Drummond et al disclose the network wherein said distributed firewall is enabled to verify the validity of said identification code submitted from a wireless access device (see Fig. 4 and 5, col. 6, line 18 to col. 9, line 22).

4. Claim 20–23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al (6,796,490) in view of Janik (6,518,724).

As per claim 20, Drummond et al disclose a wireless HUB or intelligent concentrator, comprising:

a cable connector coupled to wireless HUB and adapted to communicatively couple to a network data cable (see Fig. 4 and 5);

Art Unit: 2682

electronic circuitry mounted in wireless HUB enabled to wirelessly communicate with a wireless access device and a network ((124) has a circuit device which is IEEE802.11 or Blue-tooth or any IR to interface with wireless access device) (see Fig. 5, col. 7 lines36-51).

distributed firewall resident in said electronic circuitry wherein said firewall is enabled to control the access to said network of said wireless access device (see Fig. 4 and 5, col. 6, line 18 to col. 9, line 22).

He does not disclose an electronic circuitry mounted in a housing.

However, Janik disclose a housing (see Fig. 16, number 1600), which is used for network switching device (see Fig. 16, 17 and 23).

Therefore, at the time of the invention was made, it would have been obvious for one skilled in the art to implement the network switching device with the housing, as taught by Janik, so that the wireless devices can be protected by the housing without damaging the circuit.

As per claim 21, Drummond et al disclose the intelligent concentrator wherein said intelligent concentrator is enabled as a hub of a personal area network (see Fig. 5).

Art Unit: 2682

As per claim 22, Drummond et al does not disclose the wireless HUB wherein a list of valid ID code.

Janik disclose the list of valid identification codes is resident in switch device (see Janik, Fig. 22, col.11, lines 33-39).

Therefore, it would have been obvious for a person skilled in the art to include in the list of valid identification codes in the wireless HUB so that the wireless HUB enables to identify the valid wireless device.

As per claim 23, Drummond et al disclose said distributed firewall is enabled to verify validity of an identification code submitted by a wireless access device (see Fig. 4 and 5, col. 6, line 18 to col. 9, line 22).

5. Claim 6, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al (6,796,490) in view of Rioz et al (WO 01/17310) and further in view of Janik (6,518,724).

As per claim 6, the combination of Drummond and Rioz does not specifically disclose a list of ID code in the wireless HUB.

Janik teaches the method wherein said list of valid identification codes is resident in switch device (see Janik, Fig. 22, col.11, lines 33-39).

Art Unit: 2682

At the time of the invention was made, it would have been obvious for one skilled in the art to include in ID code, as taught by Janik, in order to track wireless device's identification code so that the system can prevent intrusion of computer hackers.

As per claims 24 and 25, the modified of Drummond and Janik disclose a wireless HUB or intelligent concentrator in claim 20, however, they do not specifically disclose to said distributed firewall is enabled to deny access and to issue an alarm to a network if ID code is not valid.

Rioz disclose that denying wireless network access to said wireless access device when said identification code is not valid (see fig. 3, page 12, lines 2-5); and

issuing an alert when said identification code is not valid (see Fig. 3, page 12, lines 5-7).

Therefore, at the time of the invention was made, it would have been obvious for one skilled in the art to implement the authentication identity, as taught by Rioz et al, in order to have a fully access network protection so that

Art Unit: 2682

computer hackers or unauthorized person can not access to the wireless network.

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Drummond et al (6,796,490).

As per claim 17, Drummond et al disclose the computer network wherein said firewall is a distributed firewall and is resident in Server; he also discloses that the wireless HUB is coupled to the server (see Fig. 5) except for said firewall in wireless HUB.

It would have been obvious for one skilled in the art at the time of the invention was made to set firewall either in the wireless HUB or in server in order to make said firewall workable, since it has been held that rearranging part of an invention involves only routine skill in the art. In re Jaspikse, 86 USPQ 70,73 (CCPA 1950).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sanh D Phu whose telephone number is (703) 305-8635. The examiner can normally be reached on 8:00-16:30.


Art Unit: 2682

The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-8635.

Sanh D. Phu
Examiner
Art Unit 2682

SP


VIVIAN CHIN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600
11/15/04